

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   3 月 3 1 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 0 9 6 0 8 8  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 0 9 6 0 8 8 ]

出   願   人            株 式 会 社 エヌ ・ ティ ・ ティ ・ ド コ モ  
Applicant(s):

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 4 年   3 月 2 6 日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出 証 番 号    出 証 特 2 0 0 4 - 3 0 2 5 4 9 3

【書類名】 特許願

【整理番号】 DCMH140848

【提出日】 平成15年 3月31日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 端末装置及びプログラム

【請求項の数】 7

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 成瀬 直樹

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 市川 裕一

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 大井 達郎

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 渡邊 信之

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 服部 易憲

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 竹下 理人

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 西田 真和

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 浅井 真生

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 津田 雅之

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 富岡 淳樹

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 山田 和宏

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ・ ティ・ ドコモ内

【氏名】 神谷 大

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 鷺尾 諭

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 山根 直樹

## 【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 村上 圭一

## 【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

## 【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

## 【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

## 【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

●

【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 端末装置及びプログラム

【特許請求の範囲】

【請求項 1】 他のファイルの予め定められた個所に格納されたデータに基づいて算出された値を表す特定のデータを格納した第 1 のファイルと、データを格納した第 2 のファイルを受信する受信手段と、

前記第 2 のファイルの前記個所に格納されたデータを予め定められた 1 方向関数に代入して値を算出する算出手段と、

前記算出手段により算出された値と前記特定のデータで表される値とを比較する比較手段と、

前記比較手段による比較結果に基づいて前記第 1 のファイルと前記第 2 のファイルとの組み合わせの正当性を判定する判定手段と  
を有する端末装置。

【請求項 2】 前記個所はファイル全体である  
ことを特徴とする請求項 1 に記載の端末装置。

【請求項 3】 前記個所はファイルの作成者を示すデータが格納される個所である

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 4】 前記第 2 のファイルは前記端末装置により実行されるプログラムを格納したファイルであり、前記第 1 のファイルは前記第 2 のファイルをダウンロードするために必要なデータを格納したファイルである

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 5】 前記第 2 のファイルは前記端末装置により実行されるプログラムを格納したファイルをダウンロードするために必要なデータを格納したファイルであり、前記第 1 のファイルは前記端末装置が前記プログラムを実行することにより実現されるアプリケーションの機能の制限に必要なデータを格納したファイルである

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 6】 前記 1 方向関数はハッシュ関数である

ことを特徴とする請求項 1 に記載の端末装置。

【請求項 7】 コンピュータ装置を、

他のファイルの予め定められた個所に格納されたデータに基づいて算出された値を表す特定のデータを格納した第 1 のファイルと、データを格納した第 2 のファイルを受信する受信手段と、

前記第 2 のファイルの前記個所に格納されたデータを予め定められた 1 方向関数に代入して値を算出する算出手段と、

前記算出手段により算出された値と前記特定のデータで表される値とを比較する比較手段と、

前記比較手段による比較結果に基づいて前記第 1 のファイルと前記第 2 のファイルとの組み合わせの正当性を判定する判定手段

として機能させるためのプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ダウンロードしたデータの正当性を判定する技術に関する。

【0 0 0 2】

【従来の技術】

近年、プログラム等のソフトウェアをインターネット等のネットワーク経由で通信端末にダウンロードして使用することが広く行われている。このような環境下でソフトウェアの改竄や「なりすまし」などの不正行為を完全に排除することは困難であるから、不正なソフトウェアが通信端末にダウンロードされてしまう虞がある。このような事情から、ダウンロードしたソフトウェアの正当性を確認するための技術が提案されている。例えば、ダウンロードするソフトウェアのハッシュ値を記録した I C (Integrated Circuit) カードを当該ソフトウェアの提供元が予めユーザに貸与する方法が提案されている (特許文献 1 参照)。この方法では、ユーザが通信端末に I C カードを装填しソフトウェアのダウンロードを指示すると、通信端末はソフトウェアをダウンロードし、ハッシュ関数を用いて当該ソフトウェアに対するハッシュ値を算出し、このハッシュ値を I C カードに

記録されたハッシュ値と比較し、両者が一致したら、受信したソフトウェアが正当であると判断する。

【0 0 0 3】

【特許文献】

特開平 1 1 - 2 0 5 7 6 7 号公報

【0 0 0 4】

【発明が解決しようとする課題】

ところで、J a v a - A P（アプリケーション）ソフトウェアをダウンロードし実行することができる携帯電話機が普及している。この種の携帯電話機へ J a v a - A P ソフトウェアをダウンロードする際には、WWW（World Wide Web）を構成するサーバ装置から A D F（Application Descrcptor File）がダウンロードされ、次いで J A R（Java Archive）ファイルがダウンロードされることになる。これらのファイルも不正行為の対象となり得るから、ダウンロードしたソフトウェアの正当性の確認が必要である。

ところで、A D F は対応する J A R ファイルの作成日付などの J A R ファイルに関する情報を内包していることから、対応する J A R ファイルが更新されると更新されねばならない。つまり、A D F と J A R ファイルには正当な組み合わせが存在する。したがって、J a v a - A P ソフトウェアの正当性の確認には、A D F 及び J A R ファイルの組み合わせの正当性の確認が必須である。

A D F 及び J A R ファイルの組み合わせの正当性を確認する方法としては、正当な組み合わせの A D F および J A R ファイルを一体化してからハッシュ値を算出し、このようなハッシュ値を特許文献に記載された技術において用いるようにする方法が考えられる。しかし、J a v a - A P ソフトウェアは、その提供者によりバグが修正されたりバージョンアップされたりするものであるから、その度にハッシュ値が変わることになる。したがって、J a v a - A P ソフトウェアの提供者である C P（Contents Provider）は、当該 J a v a - A P ソフトウェアの変更の都度、ハッシュ値を記録した I C カードを当該 J a v a - A P ソフトウェアの利用者へ配布しなければならない。これは非現実的である。

【0 0 0 5】



本発明は、上述した事情に鑑みて為されたものであり、ダウンロードした関連する複数のファイルの組み合わせの正当性を容易に判定することができる技術を提供することを目的としている。

#### 【 0 0 0 6 】

##### 【課題を解決するための手段】

上述した課題を解決するために、本発明は、他のファイルの予め定められた個所に格納されたデータに基づいて算出された値を表す特定のデータを格納した第 1 のファイルと、データを格納した第 2 のファイルを受信する受信手段と、前記第 2 のファイルの前記個所に格納されたデータを予め定められた 1 方向関数に代入して値を算出する算出手段と、前記算出手段により算出された値と前記特定のデータで表される値とを比較する比較手段と、前記比較手段による比較結果に基づいて前記第 1 のファイルと前記第 2 のファイルとの組み合わせの正当性を判定する判定手段とを有する端末装置を提供する。

また、本発明は、コンピュータ装置を、他のファイルの予め定められた個所に格納されたデータに基づいて算出された値を表す特定のデータを格納した第 1 のファイルと、データを格納した第 2 のファイルを受信する受信手段と、前記第 2 のファイルの前記個所に格納されたデータを予め定められた 1 方向関数に代入して値を算出する算出手段と、前記算出手段により算出された値と前記特定のデータで表される値とを比較する比較手段と、前記比較手段による比較結果に基づいて前記第 1 のファイルと前記第 2 のファイルとの組み合わせの正当性を判定する判定手段として機能させるためのプログラムを提供する。

#### 【 0 0 0 7 】

本発明によれば、受信手段により受信された第 2 のファイルの予め定められた個所に格納されたデータを 1 方向関数に代入して算出された値と、受信手段により受信された第 1 のファイルに格納された特定のデータで表される値とが比較され、この比較結果に基づいて前記第 1 のファイルと前記第 2 のファイルとの組み合わせの正当性が判定される。

#### 【 0 0 0 8 】

##### 【発明の実施の形態】

以下、図面を参照して、本発明の実施の一形態である配信システムについて図面を参照して説明する。なお、図面において、共通する部分には同一の符号が付されている。

この配信システムは、ユーザが、携帯電話機を操作して所望の J a v a - A P ソフトウェアを携帯電話機にダウンロードおよびインストールし、携帯電話機において起動するためのものである。

#### 【0009】

本システムにおける J a v a - A P ソフトウェアのダウンロードは、まず、携帯電話機が、J a v a - A P ソフトウェアの内容を説明した画面を表示した後、この携帯電話機のユーザが所望する J a v a - A P ソフトウェアに対応した A D F を受信し、次いで、上記 J a v a - A P ソフトウェアに対応した S D F (セキュリティ記述ファイル) と称せられるファイルを受信し、最後に J A R ファイルを受信するという手順で行われる。ここで、S D F は、携帯電話機内における J a v a - A P ソフトウェアの挙動を制限する内容が記述されたファイルである。よって、携帯電話機は、インストールした J a v a - A P ソフトウェアを実行するに際しては、この S D F の記述内容に従うこととなる。この S D F は、J a v a - A P ソフトウェアについて上記通信事業者とこの J a v a - A P ソフトウェアを提供する C P との間で結ばれた契約に従って通信事業者により作成される。

ところで、本実施形態では、対応する S D F が存在する J a v a - A P ソフトウェアと、対応する S D F が存在しない J a v a - A P ソフトウェアとが用意されている。前者の J a v a - A P ソフトウェアは、対応する S D F に記述された許可情報による挙動制限を受けるものであり、通信事業者が C P との契約に基づいて信頼性を保証したものであることから、以降の説明では、前者を「トラステッド J a v a - A P ソフトウェア」と呼ぶ。これに対応して、後者を「非トラステッド J a v a - A P ソフトウェア」と呼ぶ。

なお、本実施形態の説明において「J a v a - A P ソフトウェア」と言う場合には、それが「トラステッド J a v a - A P ソフトウェア」であれば A D F、S D F 及び J A R ファイルを含む概念とし、「非トラステッド J a v a - A P ソフトウェア」であれば A D F 及び J A R ファイルを含む概念とする。

**【0010】****(1：構成)**

図1に示されるように、この配信システムは、インターネット11に接続されたCPサーバ装置12と、通信事業者が移動パケット通信サービスを提供するために用いる移動パケット通信網15と、この移動パケット通信網15を介して通信相手とパケット通信を行う携帯電話機16と、インターネット11と移動パケット通信網15とを相互接続するゲートウェイサーバ装置17と、ゲートウェイサーバ装置17に接続されたトラステッドサーバ装置18とを有する。この配信システムには多数の携帯電話機が存在するが、図面が繁雑になるのを避けるために一つの携帯電話機16のみが図示されている。これと同様の理由により、一つのCPサーバ装置12のみが図示されている。

**【0011】**

以下、この配信システムの各構成要素について詳細に説明する。

**(1-1：CPサーバ装置)**

CPサーバ装置12は、一般的なWWWサーバ装置と同様のハードウェアおよび機能を有する。また、CPサーバ装置12はハードディスク装置12Aを有する。CPサーバ装置12は、TCP (Transmission Control Protocol) に従ったコネクション (以後、TCPコネクション) を通信相手との間に確立し、このコネクションを介してHTTP (Hypertext Transfer Protocol) のGETメソッドを用いた要求メッセージを受信すると、このGETメソッドに指定されたURL (Uniform Resource Locator) で特定されるファイルを自身のハードディスク装置12Aから読み出し、このファイルを含むHTTPの応答メッセージを送ってこのコネクションを切断する。

**【0012】**

ハードディスク装置12Aは、Javaプログラミング言語を用いて作成されたプログラムを内包するJARファイルと、このJARファイルに関する情報を記述したADFを記憶し得る。

CPサーバ装置12に記憶され得るADFには、トラステッドJava-APソフトウェアに対応したADFと、非トラステッドJava-APソフトウェア

に対応した ADF とがある。これらのいずれの ADF においても、Java-AP ソフトウェアの名称や、WWW における JAR ファイルの記憶位置を示す JAR 保存先 URL データや、JAR ファイルのサイズを示す情報や、JAR ファイルの最終変更日時を示す情報等の、従来から ADF に内包されている情報が記述されている。これに加えて、トラステッド Java-AP ソフトウェアに対応した ADF は、図 2 に示されるように、トラステッド Java-AP ソフトウェアである場合に記述されるトラステッド APID データ、SDF が WWW において記憶されている位置を示すトラステッドサーバドメインと、図示せぬ CA（認証局；Certificate Authority）から CP サーバ装置 12 を運用する CP へ提供された証明書データと、JAR ファイルのハッシュ値を表す Jar ハッシュ値データが内包されている。

ここで、ハッシュ値とは、任意のデータをハッシュ関数に代入することにより算出される一定長の算出値である。ハッシュ関数は一方向関数の一種である。

「一方向関数」とは、 $y = f(x)$  は高速に計算できるが、 $y$  から  $x$  を求める  $f$  の逆関数は存在せず、 $x$  を求めるには膨大な計算時間を要し、 $x$  を求めるのは事実上不可能な関数をいう。

また、CP サーバ装置 12 は、CP の指示に従って上記各ファイルを作成および更新する機能を備えている。また、ハードディスク装置 12A は、CP が認証局に認証されていることを証明するための、CA が発行した証明書データを記憶し得る。また、CP サーバ装置 12 は、JAR ファイルや証明書データから、SHA-1 のハッシュアルゴリズムに従ってハッシュ値を算出するプログラムを記憶し得る。

### 【0013】

（1-2：ゲートウェイサーバ装置）

ゲートウェイサーバ装置 17 は、前述の通信事業者により管理されており、移動パケット通信網 15 とインターネット 11 とを接続する一般的なゲートウェイサーバ装置と同様の構成を有し、移動パケット通信網 15 とインターネット 11 との間で相互に通信を中継する。

### 【0014】

## (1-3: トラストサーバ装置)

トラストサーバ装置 18 は前述の通信事業者により管理されており、WWW を構成し、一般的な WWW サーバ装置と同様のハードウェアおよび機能を有する。また、トラストサーバ装置 18 はハードディスク装置 18A を有し、TCP コネクションを通信相手との間に確立し、このコネクションを介して HTTP の GET メソッドを用いた要求メッセージを受信すると、この GET メソッドに指定された URL で特定されるファイルをハードディスク装置 18A から読み出し、このファイルを含む HTTP の応答メッセージを返送してこのコネクションを切断する。

## 【0015】

ハードディスク装置 18A に記憶されるファイルとしては、複数のトラスト J a v a - A P ソフトウェアに対応した複数の S D F がある。

S D F は、トラスト J a v a - A P ソフトウェア毎に通信事業者により作成されるファイルである。図 3 に示されるように、S D F は、トラスト J a v a - A P ソフトウェアが記憶されている位置を表す J A R 保存先 URL データと、対応する A D F ファイルに証明書データが内包されているか否かを表す A D F 証明書有無フラグデータと、A D F に含まれている証明書データから算出したハッシュ値を表す証明書ハッシュ値データと、トラスト J a v a - A P ソフトウェアが使用を許可されている A P I (Application Program Interface) や URL を表すパーミッション情報データとを内包している。

ここで、パーミッション情報データには、電話帳参照、未読メール取得、発着信情報取得 A P I の使用を許可するか否かを表す個人情報取得データや、着信メロディ、発着信画像、待ち受け画像登録など、携帯電話機設定更新用 A P I の使用を許可するか否かを表す設定更新データや、アクセスを許可する URL を表すアクセス許可 URL データが含まれている。

## 【0016】

## (1-4: 携帯電話機)

携帯電話機 16 は、図 4 に示されるように、OS (オペレーティングシステム) ソフトウェア、J a v a - A P を実行する環境を構築するための J a v a - A

P環境ソフトウェア、および各種ネイティブAPソフトウェア等を記憶したROM16Aと、ROM16Aからプログラムを読み出して実行するCPU16Bと、表示部16Cと、不揮発性メモリ16Dと、RAM16Eと、通信部16Fと、操作部16Gとを有し、これらはバスによって接続されている。

#### 【0017】

表示部16Cは、例えば液晶表示パネルやパネル駆動回路を有し、CPU16Bから供給されるデータで表される画像を表示する。

不揮発性メモリ16Dは、例えば、SRAM (Static Random Access Memory) やEEPROM (Electrically Erasable and Programmable Read Only Memory) である。また、この不揮発性メモリ16Dは、WWWを構成するサーバ装置からダウンロードされたJava-APソフトウェアを記憶するために使用される。

また、不揮発性メモリ16Dには、SHA-1のハッシュアルゴリズムに従って、ハッシュ値を計算するプログラムが記憶されている。

#### 【0018】

通信部16Fは、アンテナや無線送受信部を備え、移動パケット通信網15と無線パケット通信を行うものであり、CPU16Bと移動パケット通信網15との間でパケットを中継する。また、通信部16Fは、通話のためのマイク、スピーカ等を備えており、これによって携帯電話機16は図示せぬ移動電話網を介して回線交換による通話を行うこともできる。

操作部16Gは操作子を備え、操作子の操作に応じた信号をCPU16Bへ供給する。

#### 【0019】

##### (2. 動作)

次に、上述した通信システムの動作例について説明する。

携帯電話機16の図示せぬ電源が投入されると、CPU16BはRAM16Eをワークエリアとし、ROM16AからOSソフトウェアに内包されているプログラムを読み出して実行する。これにより、CPU16BにはUI (User Interface; ユーザインターフェース) 等を提供する機能が実現される。すなわち、C

P U 1 6 BはOSソフトウェアを起動して携帯電話機16内にて図5に示すOSを実現する。OSは操作部16Gから供給される信号とUIの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

#### 【0020】

例えば、ユーザの指示がJ a v a - A Pソフトウェアのダウンロードを要求するものである場合には、W e bブラウザは、この指示を次に述べるJ A M (Java Application Manager) に通知する。

また、ユーザの指示がネイティブA PソフトウェアであるJ A Mソフトウェアの起動を要求するものであれば、OSはJ A Mソフトウェアを起動して携帯電話機16内にてJ A Mを実現する。J A Mは、携帯電話機16にインストールされているJ a v a - A Pソフトウェアの一覧をユーザに提示し、ユーザにより指定されたJ a v a - A Pソフトウェアを起動する。具体的には、J A Mに対するユーザの指示がJ a v a - A Pソフトウェアの起動を要求するものであれば、J a v a - A P環境ソフトウェアが起動されて携帯電話機16内にJ a v a - A P環境が実現され、次に、指定されたJ a v a - A Pソフトウェアが起動されてJ a v a - A P環境内にJ a v a - A Pが実現される。J a v a - A P環境は、携帯電話機16のような携帯端末に適した軽量のJ a v a仮想マシンであるK V M (K Virtual Machine) と、J a v a - A Pに対して提供されるA P I (Application Interface) とを有する。J a v a - A Pに対して提供されるA P Iは、トラステッドJ a v a - A Pソフトウェアによって実現されるJ a v a - A Pに使用が許可されるS D Fのパーミッション情報データで指定されるA P Iと、あらゆるJ a v a - A Pに使用が許可される非トラステッドA P Iとに分けられる。

#### 【0021】

なお、以下に述べる動作において、T C Pコネクションの確立および切断動作についてはH T T Pにおける一般的な動作となることから、それらの説明を省略する。また、前述のOS、W e bブラウザ、J A M、J a v a - A P、ネイティブA P等が行う動作は携帯電話機16の動作となることから、以降の説明では、動作の主体を携帯電話機16とする。

**【0022】**

(2-1: トラストッド J a v a - A P ソフトウェアの作成)

まず、C P の管理する C P サーバ装置 1 2 が、トラストッド J a v a - A P ソフトウェアを作成する動作を、図 6 を参照して説明する。

ここで、C P は、予め、入力された J A R ファイルや証明書データより、S H A - 1 のハッシュアルゴリズムに従ってハッシュ値を算出するプログラム（以下、「ツール」という）を通信事業者より貸与されており、当該プログラムは、C P サーバ装置 1 2 のハードディスク装置 1 2 A に記憶されているものとする。また、C P サーバ装置 1 2 のハードディスク装置 1 2 A には、予め C A より取得した証明書データが記憶されているものとする。

**【0023】**

まず、C P は、C P が所望するアプリケーション「TELNO 別着信メロディ変更アプリ」を実現させるためのプログラムを作成し、当該プログラムを内包した J A R ファイルを“http://www.b.co.jp/ melody.jar”で特定される位置に記憶させるよう入力する。また、C P は、当該プログラムのアプリ名“melody by TELNO”を表すアプリ名データや J A R 保存先 U R L データ等の各種情報を記述した A D F を C P サーバ装置 1 2 に入力し、通信事業者より貸与されているツールを起動する指示を行う。

これにより、C P サーバ装置 1 2 の C P U は、ハードディスク装置 1 2 A よりツールを読み出し、入力された J A R ファイルより、J a r ハッシュ値データを算出する。また、C P サーバ装置 1 2 の C P U は、証明書データより、証明書データハッシュ値を算出する。そして、C P サーバ装置 1 2 の C P U は、算出した J a r ハッシュ値データと、証明書データ、アプリ名データ“melody by TELNO”、J A R 保存先 U R L データ“http://www.b.co.jp/ melody.jar”とを含んだ A D F を作成する。

そして、C P サーバ装置 1 2 は、トラストッドサーバ装置 1 8 に、作成した A D F、J A R ファイル、証明書データハッシュ値とを送信する（ステップ S 1）。

**【0024】**



トラステッドサーバ装置 18 を所有する通信事業者は、上記ファイルを受信した後、まず、当該ファイルを作成した CP の安全性を審査する。

具体的には、通信事業者は、ADF に内包されている証明書データは、通信事業者が認めた正当な CA から発行されているか、証明書が複数の CA から発行されている場合には、当該複数の証明書によって構成される証明書チェーンは正当であるか、チェーンの上位の認証機関は通信事業者が認めた CA であるか等の検証を行う。

次に、通信事業者は、CP が作成した Java-AP ソフトウェアの安全性を審査する。具体的には、例えば、通信事業者は、JAR ファイルのプログラム記述を検査することにより、当該 Java-AP ソフトウェアにより実現されるアプリケーションが、携帯電話機 16 に記憶されている個人情報を破壊したり、個人情報を流出させたりする可能性があるか否かを審査する。

そして、通信事業者は、上記検証結果、検査結果を基に、Java-AP ソフトウェアが使用可能な API や URL を表すパーミッション情報を決定する。通信事業者は、これらのデータをトラステッドサーバ装置 18 に入力する。

#### 【0025】

トラステッドサーバ装置 18 の CPU は、CP サーバ装置 12 より受信した ADF、JAR ファイルに対応する SDF を生成する。

具体的には、CPU は、ADF ファイルから読み出した “http://www.b.co.jp/melody.jar” を表す JAR 保存先 URL データと、“YES” を表す ADF 証明書フラグデータと、CP サーバ装置 12 より受信した証明書ハッシュ値データと、通信事業者によって入力されたパーミッション情報データとを含んだ SDF を生成する。

#### 【0026】

次に、トラステッドサーバ装置 18 の CPU は、受信した ADF に、トラステッド Java-AP ソフトウェアを識別するためのトラステッド APID データ “0001” と、対応する SDF が記憶されているトラステッドサーバ装置 18 における位置を特定するためのトラステッドサーバドメインデータ “http://www.a.co.jp/melody.sdf” を付加する。そして、CPU は、当該データを付加した

ADFをCPサーバ装置12に送信する（ステップS2）。

【0027】

CPサーバ装置12のCPUは、ADFを受信して、自装置のハードディスク装置12Aに当該ADFを記憶する。これにより、Java-APソフトウェアは携帯電話機16よりダウンロード可能な状態となる。

【0028】

（2-2：携帯電話機16によるJava-APソフトウェアのダウンロード）

次に、ユーザが携帯電話機16を用いて、Java-APソフトウェアのダウンロードの指示を行ったときの動作を、図6を参照して説明する。

ここでは、上記2-1：トラステッドJava-APソフトウェアの作成処理が行われてから、ADF、JARファイルの内容は、変更されていないものとする。

【0029】

ユーザは、携帯電話機16の操作部16Gを操作して、CPサーバ装置12よりトラステッドJava-APソフトウェア「TELNO別着信メロディ変更アプリ」をダウンロードする指示を行う。

CPU16Bは、上記トラステッドJava-APソフトウェアのダウンロードを要求する指示がWebブラウザから通知されると、当該トラステッドJava-APソフトウェアを携帯電話機16にダウンロードする処理を行う。

まず、CPU16Bは、ダウンロードしようとするJava-APソフトウェアに対応するADFをCPサーバ装置12から取得する。具体的には、CPU16Bは、CPサーバ装置12との間にTCPコネクションを確立し、このADFの送信を要求する内容の要求メッセージを生成・送信し（ステップS3）、このメッセージに対する応答メッセージを受信してADFを取得した後（ステップS4）、このTCPコネクションを切断する。そして、CPU16Bは、応答メッセージに内包されているADFを不揮発性メモリ16Dに書き込む。

【0030】

次いで、CPU16Bは、ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであるか否かを判定する。具体

的には、CPU16Bは、受信したADF内にトラステッドAPIDデータが記述されているか否かを確認し、記述されていれば、このJava-APソフトウェアに対応するSDFが存在する、即ち、トラステッドJava-APソフトウェアであると判定し、その記述がなければ非トラステッドJava-APソフトウェアであると判定する。

#### 【0031】

そして、ダウンロードしようとするJava-APソフトウェアが非トラステッドJava-APソフトウェアであると判定された場合には、ADFに内包されているJAR保存先URLデータで特定されるURLで表される位置より、JARファイルがダウンロードされ、従来と同様のダウンロード処理が行われる。

#### 【0032】

ここでは、トラステッドAPIDデータに“0001”を表すデータが記述されているので、CPU16Bは、ダウンロードしようとするJava-APソフトウェアがトラステッドJava-APソフトウェアであると判定し、ADFに内包されているトラステッドサーバドメインデータで表されるURL “http://www.a.co.jp/melody.sdf”で特定される位置より、このソフトウェアに対応するSDFを取得する。すなわち、CPU16Bは、トラステッドサーバ装置18との間にTCPコネクションを確立し、このコネクションを介して、ADF内に内包されているトラステッドサーバドメインデータで表されるURL “http://www.a.co.jp/melody.sdf”で特定されるSDFの送信をトラステッドサーバ装置18に要求する内容の要求メッセージを生成・送信する（ステップS5）。CPU16Bは、このメッセージに対する応答メッセージを受信してSDFを取得した後（ステップS6）、上記コネクションを切断する。

#### 【0033】

次に、携帯電話機16がSDFを受信してからトラステッドJava-APソフトウェアを検証する処理の動作を、図7を参照して説明する。

まず、CPU16Bは、ADFに証明書データが内包されているか否かを判定する（ステップS101）。具体的には、受信したSDFに内包されているADF証明書有無フラグデータが、“Yes”を表すデータか否かを判定する。AD

Fに証明書データが内包されていないと判定された場合には（ステップS101；No）、証明書データの検証は行わずに、JARファイルのダウンロードを行う（ステップS104）。

#### 【0034】

ここでは、ADF証明書有無フラグデータが“Yes”を表すデータであるため、CPU16Bは、ADFに証明書データが内包されていると判定し（ステップS101；Yes）、ADFに内包されている証明書データのハッシュ値を算出する（ステップS102）。

そして、CPU16Bは、ADFに内包されている証明書データから算出したハッシュ値と、SDFに予め内包されている証明書ハッシュ値データで表される証明書ハッシュ値とを比較し、一致しているか否か判定する（ステップS103）。一致していない場合には（ステップS103；No）、通信事業者がSDFを作成した時点以降に、ADFに内包されている証明書データが変更されている可能性があるため、ユーザにダウンロード失敗の通知を行うと共に、CPU16BはADFを削除して、携帯電話機16をADFダウンロードする前の状態に戻し（ステップS107）、処理を終了する。

#### 【0035】

ここでは、ハッシュ値は一致しているため（ステップS103；Yes）、CPU16Bは、JARファイルをダウンロードする（ステップS104）。具体的には、CPU16Bは、ADFに内包されているJAR保存先URLデータで表されるURL“http://www.b.co.jp/melody.jar”で特定されるJARファイルを記憶したCPサーバ装置12との間にTCPコネクションを確立し、このJARファイルの送信を要求する内容の要求メッセージを生成・送信し（図6のステップS7）、このメッセージに対する応答メッセージを受信してJARファイルを取得し（図6のステップS8）、このTCPコネクションを切断する。

#### 【0036】

次に、CPU16Bは、ダウンロードしたJARファイルのハッシュ値を算出する（ステップS105）。そして、CPU16Bは、算出したハッシュ値と、ADFファイルに内包されているJarハッシュ値データで表されるハッシュ値

とを比較し、ハッシュ値が一致しているか否かを判定する（ステップS106）。ハッシュ値が一致していない場合には（ステップS106; No）、JARファイルが作成された時点以降に、JARファイルが改竄、変更等されている可能性があるため、CPU16Bは、ダウンロードに失敗した旨をユーザに通知するとともに、ダウンロードしたJARファイルとADFとを削除して携帯電話機16の状態をADFダウンロード以前の状態に戻し（ステップS108）、処理を終了する。

#### 【0037】

ここでは、ハッシュ値が一致しているため（ステップS106; Yes）、CPU16Bは、Java-APソフトウェア取得に成功した旨をユーザに通知すると共に、取得したJARファイル、SDFを不揮発性メモリ16Dに書き込み（ステップS109）、処理を終了する。

以降、CPU16は、トラステッドJava-APソフトウェア「TELNO別着信メロディ変更アプリ」を実行するに際し、JAMによって、トラステッドJava-APの挙動を監視し、パーミッション情報データに含まれる個人情報取得データ、設定更新データ、アクセス許可URLデータによって、電話帳参照API、移動機設定更新用API、URL等の使用を許可／制限する。

#### 【0038】

以上説明したように、本実施形態によれば、ADFに内包されている証明書データから算出したハッシュ値と、予めSDFに算出して記憶しておいたADFに内包されていた証明書データのハッシュ値とが一致しているのを確認することによって、通信事業者がCPから申請された証明書データを検証／許可した後にADF内の証明書データが変更、改竄されていないことを確認することができる。つまり、SDFとADFとの組み合わせの正当性を判定することができる。なお、ADF内の証明書データが同一の証明書データで上書きされた場合にはハッシュ値が一致することになり、ADFがSDF作成時のADFと異なる場合にもSDFとADFとの組み合わせが正当であると判定されることになる。つまり、上記の検証／許可の後にCPがADFを変更しても、SDFとADFとの組み合わせは正当と判定される。換言すれば、SDFとADFとの組み合わせについては

広い意味での正当性が判定される。これにより、CPは、バグフィックス等のためにCPがJARファイル及びADFを変更しても、上記の検証／許可をやり直さなくてよい。

また、本実施形態によれば、JARファイルから算出したハッシュ値と、予めADFに算出して記憶しておいたJARファイルのハッシュ値とが一致していることを確認することによって、ADFとJARファイルとの組み合わせの正当性を判定することができる。これにより、例えば、第3者によって改竄されたJARファイルの起動を禁止したりすることができる。

また、本実施形態によれば、記録媒体を予め配布したりせずとも、移動機において、ファイルの組み合わせの正当性を判定することができる。

このように、本実施形態によれば、ダウンロードした関連するADF、SDF及びJARファイルの組み合わせの正当性を容易に判定することができる。

また、ハッシュ値の算出処理は公開鍵を用いた一般的な認証処理に比較して遥かに軽いから、本実施形態によれば、移動機のように情報処理能力が低い装置であっても、組み合わせの正当性の判定を容易に行うことができる。

#### 【0039】

##### (3：変形例)

本発明は上述した実施形態に限定されず、以下のような種々の変更が可能である。

#### 【0040】

(1) 上記実施形態においては、ADFに内包されている証明書データのハッシュ値をこのADFに対応するSDFに内包させる一方、携帯電話機16においてADFの証明書データのハッシュ値を算出し、これら両者を比較してSDFとADFの対応関係の正当性を確認するようにしていたが、ADF内の証明書データ以外のデータのハッシュ値を用いるように実施形態を変形してもよい。例えば、ADF全体のハッシュ値を用いるようにしてもよい。

また、同様に、上記の実施形態においては、JARファイルのハッシュ値をこのJARファイルに対応するADFに内包させる一方、携帯電話機においてJARファイルのハッシュ値を算出し、これら両者を比較してJARファイルとAD

Fとの対応関係の正当性を確認するようにしていたが、例えば、JARファイルの一部のハッシュ値を用いるように実施形態を変形してもよい。

#### 【0041】

(2) 上記実施形態においては、SHA-1のアルゴリズムによるハッシュ関数を用いてハッシュ値を算出することにより、ダウンロードした関連する複数のファイルの正当性を判定したが、用いるハッシュ関数は、これに限定されない。例えば、MD5のアルゴリズムによるハッシュ関数を用いてもよい。また、ハッシュ関数に限らず、任意の一方向関数を用いることができる。

#### 【0042】

(3) 上記実施形態においては、移動機において判定を行うプログラムをROMに記憶させておくようにしたが、EEPROMに記憶させておくようにしてもよいし、移動機通信網を介してダウンロードしてEEPROMに書き込むようにしてもよい。また、当該プログラムを記録した記録媒体を移動機に装着し、このプログラムを移動機が実行するようにしてもよい。

#### 【0043】

(4) 上記実施形態においては、トラステッドサーバドメインデータをADF内に内包させて、トラステッドJava-APソフトウェアに対応するSDFを特定するようにしたが、SDFを特定する方法はこれに限定されない。例えば、トラステッドサーバ装置18を特定するためのURLを表すデータを予め携帯電話機16に記憶させておき、トラステッドサーバ装置18にSDFの送信を要求するための要求メッセージを作成する際に、トラステッドサーバ装置18を特定するためのURLを表すデータと、当該URLにおいてトラステッドJava-APソフトウェアに対応するSDF（のファイル名）を識別するためのトラステッドAPIDデータとを内包させることによって、SDFを特定するようにしてもよい。

#### 【0044】

##### 【発明の効果】

本発明によれば、ダウンロードした関連する複数のファイルの組み合わせの正当性を判定することができる。

**【図面の簡単な説明】**

【図 1】 本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

【図 2】 同システムに特有の A D F のデータ構成を示す概念図である。

【図 3】 同システムにおいてトラステッドサーバ装置に記憶されている S D F のデータ構成を示す概念図である。

【図 4】 同システムを構成する携帯電話機の構成を示すブロック図である。

【図 5】 同携帯電話機の機能構成を示す概念図である。

【図 6】 本発明の実施形態におけるデータの流れを示すためのシーケンスーチャートである。

【図 7】 同携帯電話機の検証処理の流れを示すためのフローチャートである。

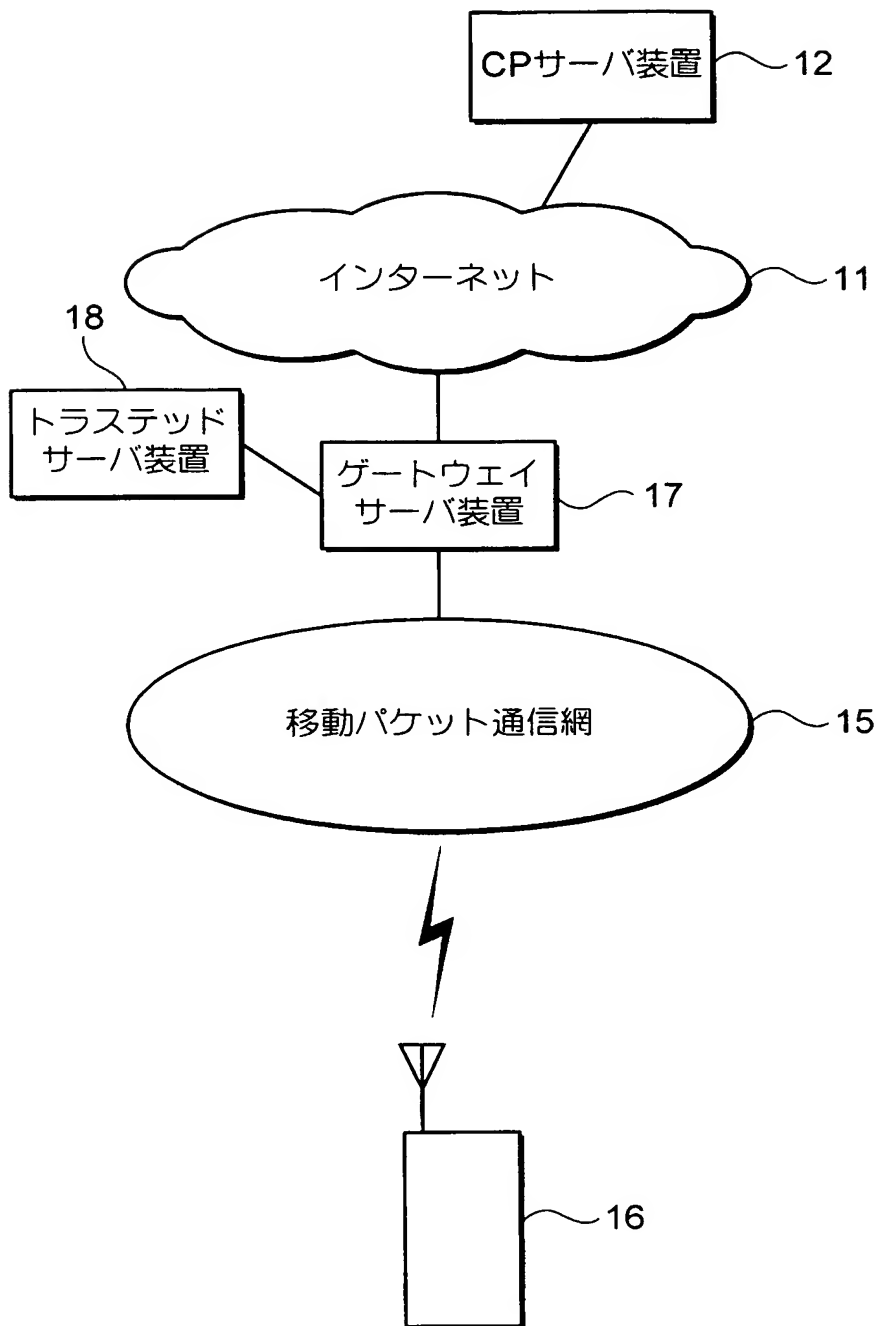
**【符号の説明】**

1 1 インターネット、1 2 C Pサーバ装置、1 5 移動パケット通信網、1 6 携帯電話機、1 7 ゲートウェイサーバ装置、1 8 トラステッドサーバ装置、1 6 D 不揮発性メモリ、1 6 A R O M、1 6 B C P U、1 6 C 表示部、1 6 E R A M、1 6 F 通信部、1 6 G 操作部。



【書類名】 図面

【図 1】



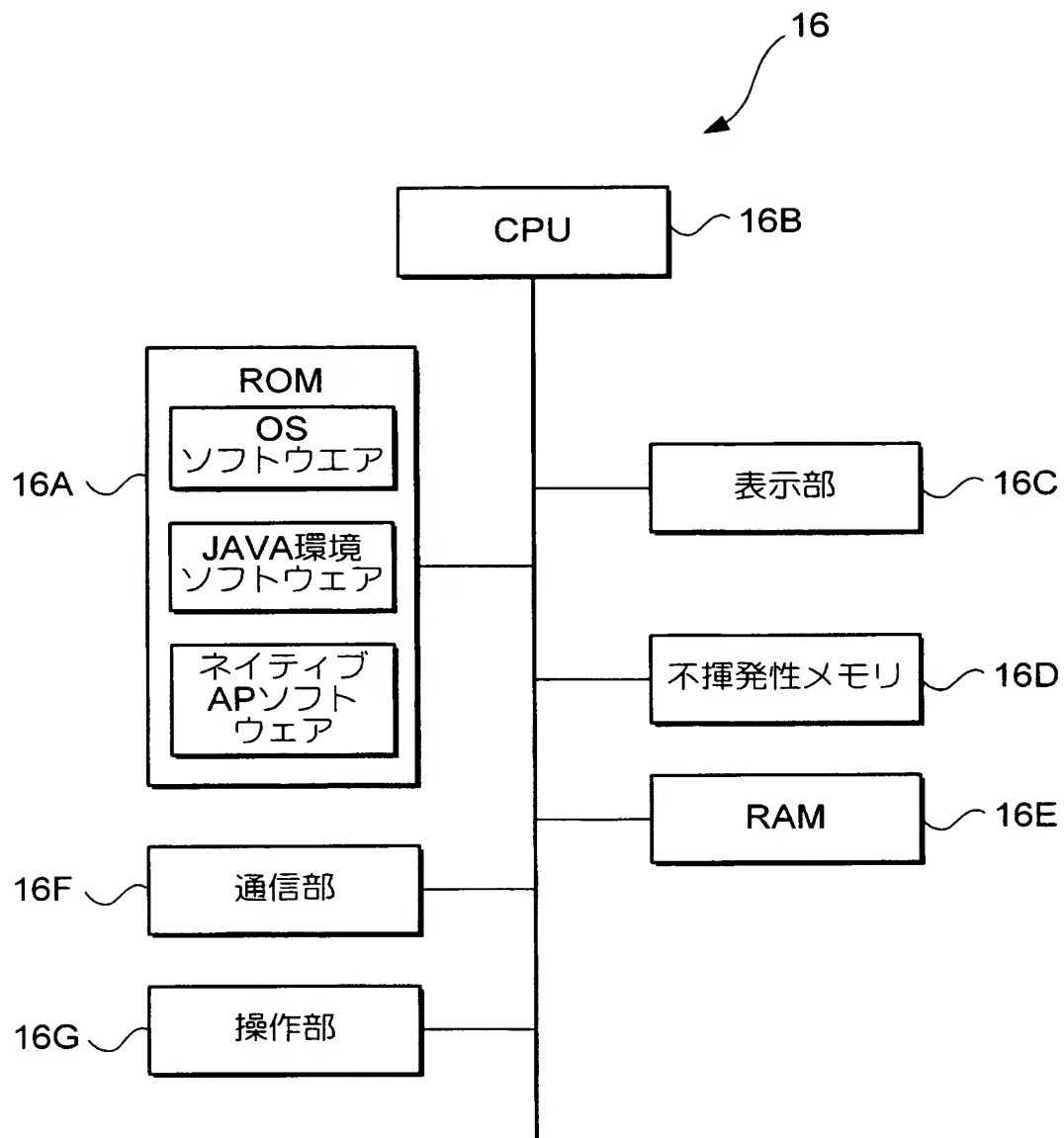
【図 2】

アプリ名
JAR保存先URL
アプリサイズ
．．．．
最終更新日
トラステッドAPID
トラステッドサーバドメイン
証明書
Jar/ハッシュ値

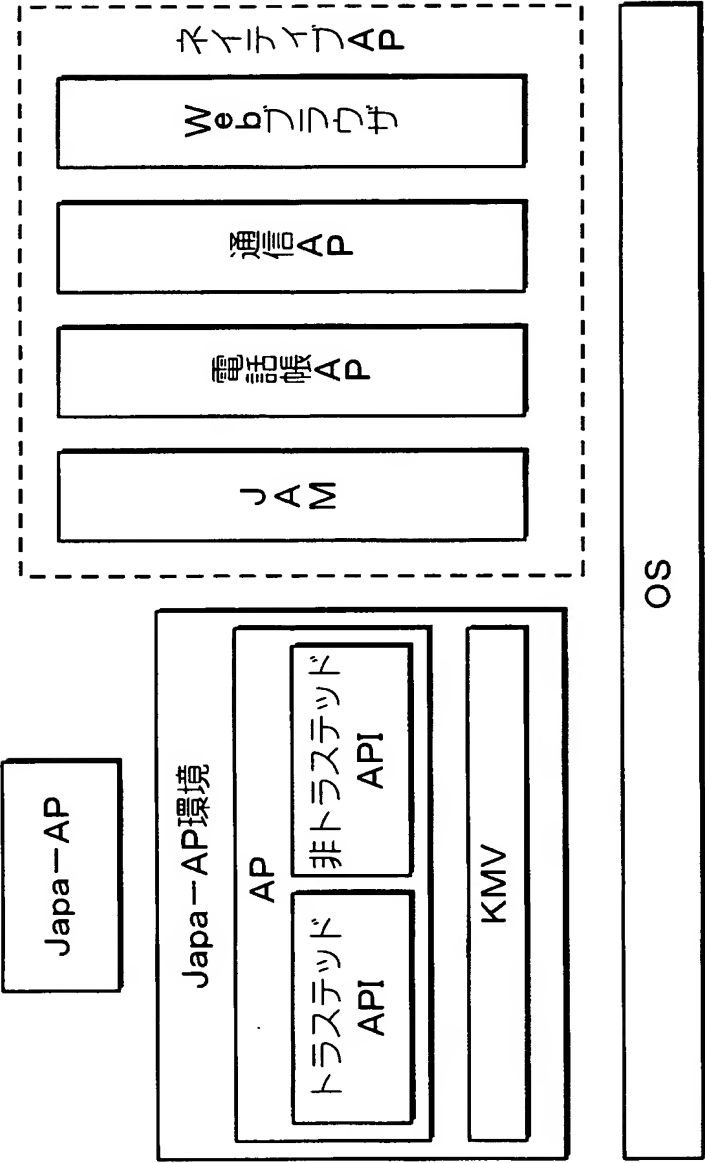
【図 3】

JAR保存先URL	
ADF証明書有無フラグ	
証明書ハッシュ値	
パー ミッション 情報	個人情報取得
	設定更新
	アクセス許可URL

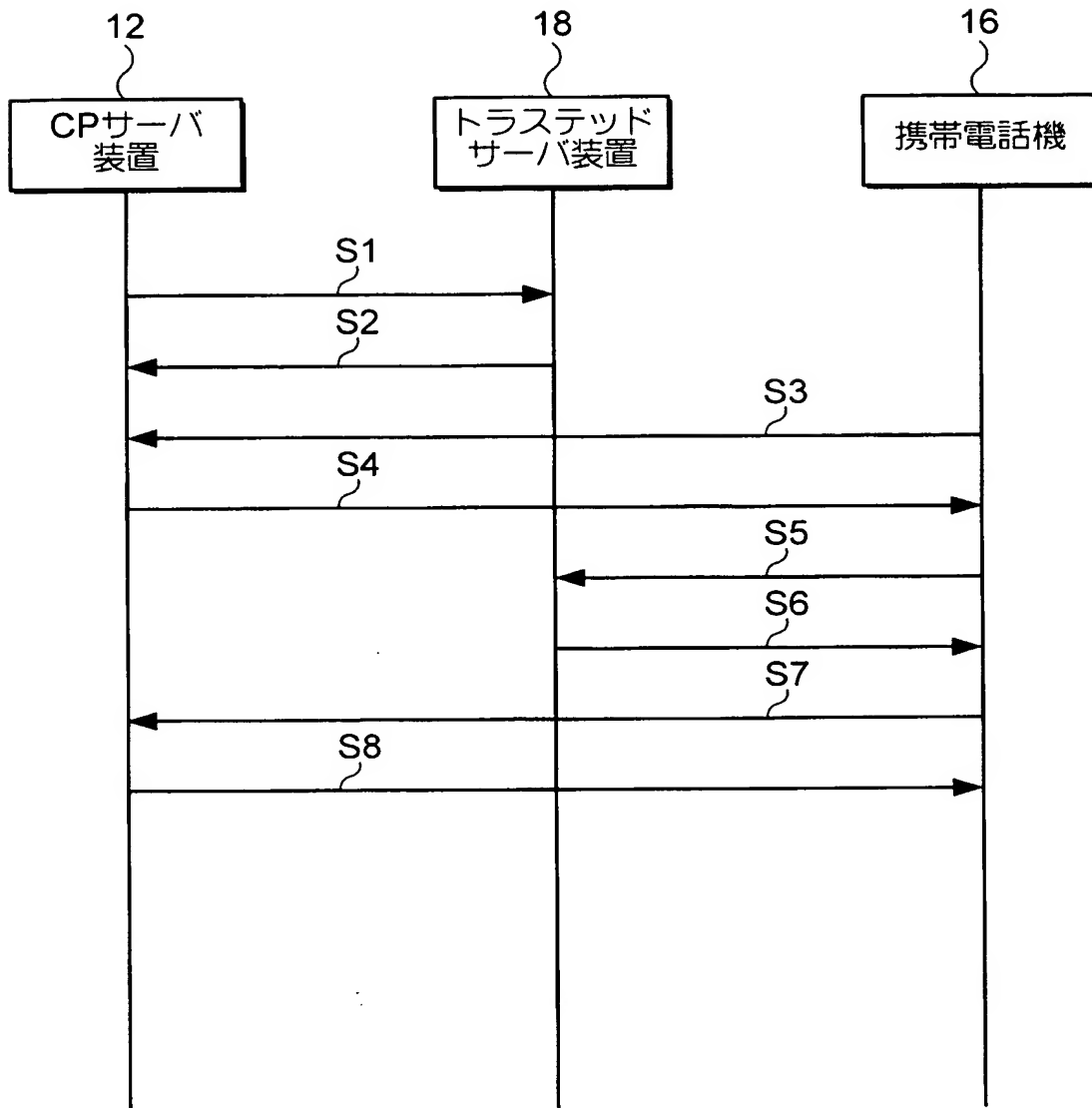
【図 4】



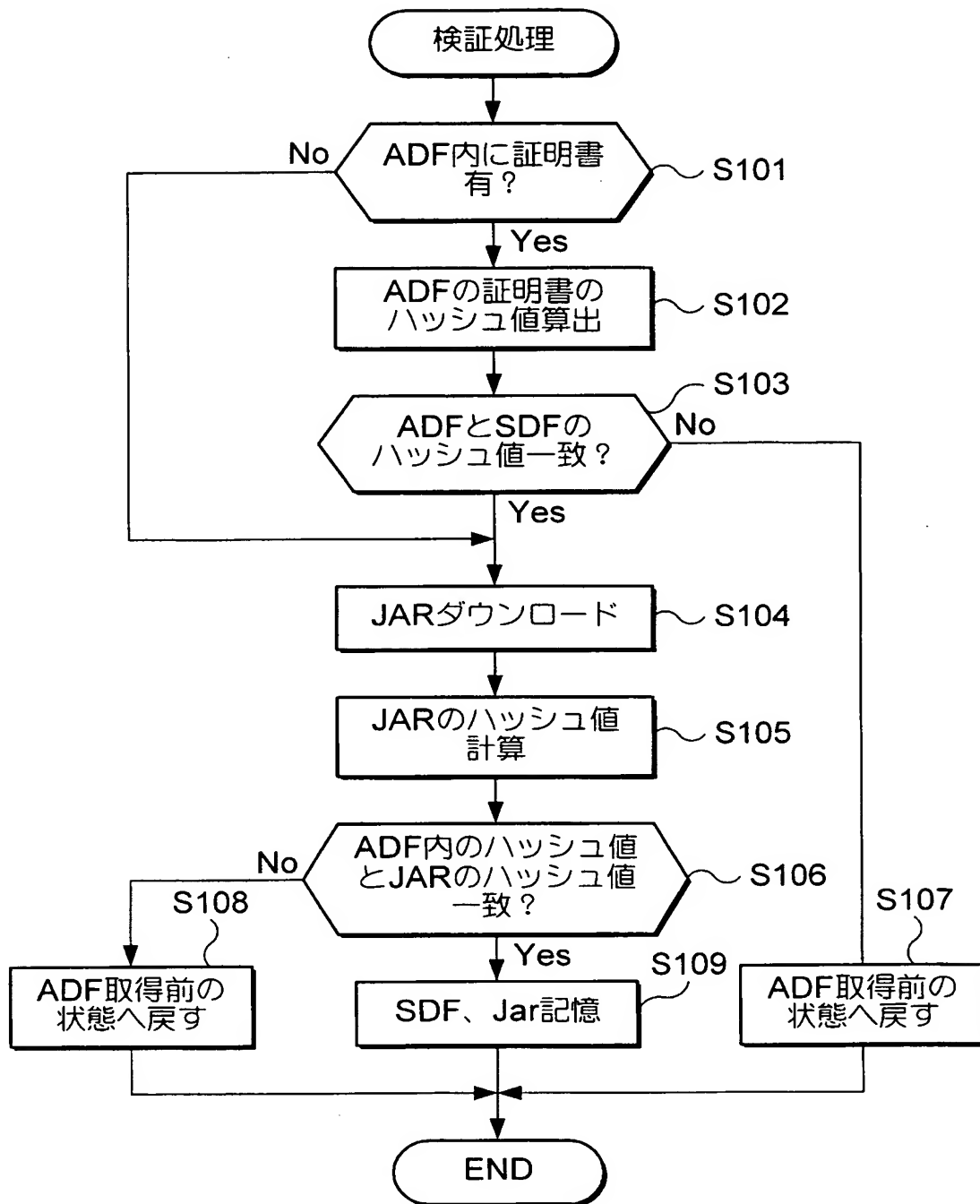
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 本発明は、ダウンロードした関連する複数のファイルの組み合わせの正当性を容易に判定することができる技術を提供する。

【解決手段】 J a v a - A P ソフトウェアを起動することができる携帯電話機 16 が、C P サーバ装置 12 から A D F を取得し、この A D F を用いてトラステッドサーバ装置 18 から S D F を受信し、A D F に内包されている証明書データから算出したハッシュ値と S D F に内包されている予め算出しておいたハッシュ値とが一致していることを確認する。次いで、携帯電話機 16 は、C P サーバ装置 12 から J A R ファイルを取得し、J A R ファイルから算出したハッシュ値と A D F に内包されている予め算出しておいたハッシュ値とが一致していることを確認する。

【選択図】 図 1



特願 2 0 0 3 - 0 9 6 0 8 8

出 願 人 履 歴 情 報

識別番号

[ 3 9 2 0 2 6 6 9 3 ]

1. 変更年月日  
[変更理由]

2 0 0 0 年 5 月 1 9 日

名称変更

住所変更

住 所  
氏 名

東京都千代田区永田町二丁目 1 1 番 1 号  
株式会社エヌ・ティ・ティ・ドコモ